IT POLICY

These are the rules, guidelines, and procedures that our organization has in place to govern the IT resources, hardware, software, data, and network.

1. **Access Control** – only authorized users can have access to the organization's IT resources, hardware, software, data, and network.
2. **Bringing Own Device to Work** – an individual can bring their own device to work, but company software must be installed to protect the organization from malicious software.
3. **Social Media** – under no circumstances should the organization's property (i.e. software, hardware, data) should be on any social media platform. This could lead to legal and cybersecurity risks.
4. **User accounts and passwords** – each individual will have their own account and password(s). If an individual is no longer a part of the organization, then their account will be deleted. Passwords must be updated every ninety (90) days to ensure protection from hackers.
5. **Backing Up Information** – information from devices will be routinely backed up every fifteen (15) days to ensure that information is not lost in case of a cyber-attack. It is also to maintain the integrity of the organization's IT resources.
6. **Purchase and Installation of Software** – All hardware and software must be appropriate and provide value for the organization. It must be able to integrate within the other devices of the organization. If an installation or purchase must occur, then it must go through the IT manager for approval. From there, the IT manager will send the approval to the IT team, who will buy it and have it installed from a reliable and authorized vendor.
7. **Incident Response** – If you see or receive something out of the ordinary, identify the incident and then report it. The incident will be properly escalated to the appropriate personnel to handle and respond to the incident. Once the incident has been dealt with, then an evaluation of the incident must occur in order to see how well it worked and whether anything else must be done to properly manage the incident.
8. **Wireless Use** – to maintain regulation of wireless network access to the organization's IT resources. User authentication is required before accessing the organization's wireless networks. The organization monitors all wireless network to ensure reliable access. The organization reserves the right to restrict and/or move any device(s) that have access to the wireless network to prevent infection or any negative impacts to the IT resources.
9. **Security Awareness and Training** – should be administered to all individuals of the organization so they can properly handle tasks without jeopardizing the organization's information and data. Providing proof of completion is required.
10. **Data Retention** – all data retrieved from the organization will be stored for three (3) years. After the three (3) years, the data will be completed destroyed and wiped from

the organization’s backup and storage. All outdated and duplicate data will be removed to keep storage space available. Data includes documents, records, transaction information, contracts, emails or other messaging applications, and customer information.

11. **Email Usage** – Personal use of company email is not allowed. This reduces the risk of receiving spam email that could contain phishing or pharming content. Email exchange must be done on-premise or using a virtual machine to access user’s desktop. In case of an email security breach, the IT manager and supervisor must be notified. The organization has the right to monitor, read, intercept, store, and disclose emails.
12. **Data and Information Security** – The availability, integrity, and confidentiality of the organization’s information must be protected from corruption, theft, or unauthorized access.